ABSTRACT

The present invention is a methodology for predicting when current sets of encryption keys used in a high speed data network are about to expire. The invention allows network elements of a communication system to re-negotiate new sets of keys well in advance so as to prevent interruptions in communications traffic flow. In accordance with one exemplary embodiment of the invention, a weighted traffic flow per usage for a given network element is calculated on a periodic basis. The value of the weighted traffic flow per usage is compared with a remainder value of a specific quantity of communications traffic yet to be processed by the network element. If the remainder value is less than the weighted traffic flow value, an indication is given to the appropriate network element to renegotiate a new set of keys.